Abstract: The NENA ESInet-PSBN Interconnection Standard contains specifications and information on connecting Emergency Services IP Networks to Public Safety Broadband Networks to support interoperable communications between Public Safety agencies and responders.
1 Executive Overview

This document contains specifications and information critical to interconnecting Emergency Services IP networks (ESInets) to Public Safety Broadband Networks (PSBNs) in a way that maximizes interoperability on both sides of the network boundary. In the context of this document, ESInets may exist at the state, regional, or local agency level. The term “PSBN” is used to refer to any broadband network that is hosting Public Safety responder devices and applications. The interconnection issues covered in this document are the same regardless of the specific ESInet or PSBN being connected. The solutions for some issues, however, are highly implementation dependent. This document provides information and advice on those types of issues.

The target audience for this document includes those who are responsible for designing and configuring the interconnect between an ESInet and PSBN (sometimes referred to as the “interconnect architect”), and those responsible for managing the relationships with network, device, and application vendors on both sides of the network interconnect. While this document is focused primarily on the network interconnect, it covers PSAP, responder, and device characteristics, as well as application interfaces when required.

Properly implemented, the standards and recommendations included in this document will enhance interoperability across key sectors of the public safety ecosystem. In particular, data and information sharing between the general public requesting emergency services, the PSAP answering their initial requests, and the first responders dispatched to address the emergency will be enabled and enhanced by implementing this standard. ESInet to PSBN interconnection and interoperability is needed to enable the promise of Next Generation 9-1-1 (NG9-1-1) and NG9-1-1 public safety in general, so proper implementation of this standard will have significant technical impact on the implementation of NG9-1-1.
# Table of Contents

1 EXECUTIVE OVERVIEW ........................................................................................................... 2

DOCUMENT TERMINOLOGY ........................................................................................................ 6

INTELLECTUAL PROPERTY RIGHTS (IPR) POLICY ................................................................. 7

REASON FOR ISSUE/REISSUE .................................................................................................. 7

2 INTERFACE SPECIFICATIONS ............................................................................................... 8

2.1 IP ADDRESSING ISSUES ...................................................................................................... 8

  2.1.1 Common Addressing Scheme ....................................................................................... 8

  2.1.2 NAT ............................................................................................................................. 8

2.2 INTERCONNECT AVAILABILITY ......................................................................................... 8

  2.2.1 Redundant Geo-diverse Connections ........................................................................ 11

  2.2.2 Physical Diversity ........................................................................................................ 11

  2.2.3 Provider Diversity ....................................................................................................... 12

  2.2.4 Failure Mitigation ....................................................................................................... 12

2.3 IDENTITY, AUTHENTICATION, AND ACCESS .................................................................. 12

  2.3.1 Identity ........................................................................................................................ 12

  2.3.2 Data Rights Management ......................................................................................... 14

2.4 PRIVACY AND INTEGRITY PROTECTION ......................................................................... 14

2.5 DIGITAL SIGNATURES ......................................................................................................... 15

  2.5.1 Data Alteration Protection ......................................................................................... 16

2.6 DATA AND MEDIA INTEROPERABILITY ............................................................................. 16

  2.6.1 Call Media .................................................................................................................. 16

  2.6.2 Responder Data Services (RDS) .............................................................................. 18

  2.6.3 Media Proxy ............................................................................................................... 18

  2.6.4 Multicast Video Support ............................................................................................ 19

2.7 PEERING ISSUES .............................................................................................................. 19

  2.7.1 Network-to-Network Interface (NNI) .................................................................... 19

  2.7.2 Maintaining Quality of Service (QoS) Across the NNI .......................................... 20

2.8 LOGGING AND CHAIN OF CUSTODY ................................................................................. 22

3 NENA REGISTRY SYSTEM (NRS) CONSIDERATIONS ......................................................... 22

4 DOCUMENTATION REQUIRED FOR THE DEVELOPMENT OF A NENA XML SCHEMA ........ 22

5 IMPACTS, CONSIDERATIONS, ABBREVIATIONS, TERMS, AND DEFINITIONS ...................... 22

  5.1 OPERATIONS IMPACTS SUMMARY ............................................................................. 22

  5.2 TECHNICAL IMPACTS SUMMARY .............................................................................. 23

  5.3 SECURITY IMPACTS SUMMARY ................................................................................. 23

  5.4 RECOMMENDATION FOR ADDITIONAL DEVELOPMENT WORK ................................ 23

  5.5 ANTICIPATED TIMELINE ............................................................................................. 23

  5.6 COST FACTORS ............................................................................................................. 23

  5.7 COST RECOVERY CONSIDERATIONS ......................................................................... 23

10/14/2021

Page 3 of 33

© Copyright 2021 National Emergency Number Association, Inc.
5.8 ADDITIONAL IMPACTS (NON-COST RELATED) ........................................................................... 24
5.9 ABBREVIATIONS, TERMS, AND DEFINITIONS .......................................................... 24

6 REFERENCES .......................................................................................................................... 28

7 EXHIBIT X ............................................................................................................................. 31

8 APPENDIX ............................................................................................................................. 31

ACKNOWLEDGEMENTS ......................................................................................................... 32
NENA STANDAR Document NOTICe

This Standard Document (STA) is published by the National Emergency Number Association (NENA) as an information source for 9-1-1 System Service Providers, network interface vendors, system vendors, telecommunication service providers, and 9-1-1 Authorities. As an industry Standard it provides for interoperability among systems and services adopting and conforming to its specifications.

NENA reserves the right to revise this Standard Document for any reason including, but not limited to:

- Conformity with criteria or standards promulgated by various agencies,
- Utilization of advances in the state of the technical arts,
- Reflecting changes in the design of equipment, network interfaces, or services described herein.

This document is an information source for the voluntary use of communication centers. It is not intended to be a complete operational directive.

It is possible that certain advances in technology or changes in governmental regulations will precede these revisions. All NENA documents are subject to change as technology or other influencing factors change. Therefore, this NENA document should not be the only source of information used. NENA recommends that readers contact their 9-1-1 System Service Provider (9-1-1 SSP) representative to ensure compatibility with the 9-1-1 network, and their legal counsel, to ensure compliance with current regulations.

Patents may cover the specifications, techniques, or network interface/system characteristics disclosed herein. No license is granted, whether expressed or implied. This document shall not be construed as a suggestion to any manufacturer to modify or change any of its products, nor does this document represent any commitment by NENA, or any affiliate thereof, to purchase any product, whether or not it provides the described characteristics.

By using this document, the user agrees that NENA will have no liability for any consequential, incidental, special, or punitive damages arising from use of the document.

NENA’s Committees have developed this document. Recommendations for changes to this document may be submitted to:

National Emergency Number Association
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202.466.4911
or commleadership@nena.org
NENA: The 9-1-1 Association improves 9-1-1 through research, standards development, training, education, outreach, and advocacy. Our vision is a public made safer and more secure through universally-available state-of-the-art 9-1-1 systems and better-trained 9-1-1 professionals. Learn more at nena.org.

Document Terminology

This section defines keywords, as they should be interpreted in NENA documents. The form of emphasis (UPPER CASE) shall be consistent and exclusive throughout the document. Any of these words used in lower case and not emphasized do not have special significance beyond normal usage.

1. MUST, SHALL, REQUIRED: These terms mean that the definition is a normative (absolute) requirement of the specification.

2. MUST NOT: This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.

3. SHOULD: This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

4. SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

5. MAY: This word, or the adjective "OPTIONAL", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option “must” be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option “must” be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

These definitions are based on IETF RFC 2119.
Intellectual Property Rights (IPR) Policy

NOTE – The user’s attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, NENA takes no position with respect to the validity of any such claim(s) or of any patent rights in connection therewith. If a patent holder has filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license, then details may be obtained from NENA by contacting the Committee Resource Manager identified on NENA’s website at www.nena.org/ipr.

Consistent with the NENA IPR Policy, available at www.nena.org/ipr, NENA invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard.

Please address the information to:

National Emergency Number Association
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202.466.4911
or commleadership@nena.org

Reason for Issue/Reissue

NENA reserves the right to modify this document. Upon revision, the reason(s) will be provided in the table below.

<table>
<thead>
<tr>
<th>Document Number</th>
<th>Approval Date</th>
<th>Reason For Issue/Reissue</th>
</tr>
</thead>
<tbody>
<tr>
<td>NENA-STA-031.1-2021</td>
<td>10/14/2021</td>
<td>Initial Document</td>
</tr>
</tbody>
</table>

10/14/2021
2 Interface Specifications

2.1 IP Addressing Issues

2.1.1 Common Addressing Scheme
All Next Generation 9-1-1 Core Services (NGCS) Functional Elements (FEs) within an ESInet are required to support both IPv4 and IPv6 interfaces. The ESInet-PSBN interconnection MUST support IPv6. The ESInet uses dynamic IP addresses obtained via the Dynamic Host Configuration Protocol (DHCP). The NENA i3 Standard for Next Generation 9-1-1 (NENA-STA-010, [53]) recommends that all elements in the ESInet have a publicly addressable IP address but does not require it. However, STA-010 requires that any entity that needs to accept connections from outside the local ESInet domain possess a publicly routable address. The Data and Media Interoperability section of this document describes some Functional Elements (FEs) that need to accept connections from responder devices on the PSBN. The Domain Name System (DNS) is an integral part of the NGCS. Hostnames, instead of IP addresses, are used to address elements in the ESInet because IP addresses change. The ESInet-PSBN interconnection MUST expect responder applications to use hostnames in connection requests and support name resolution.

2.1.2 NAT
The ESInet supports Network Address Translation (NAT) per RFC 2663 [2] due to the scarcity of IPv4 addresses. While use of NAT is discouraged within an ESInet by NENA-STA-010, NAT MUST be supported at an interconnection between peer networks like the ESInet-PSBN boundary. The use of NAT can be problematic for applications like the Session Initiation Protocol (SIP, RFC 3261 [3]) that is used extensively in the ESInet. Therefore, STA-010 requires elements in an ESInet that implement SIP interfaces to comply with RFC 5626 [4] (Outbound) to maintain connections from User Agents. Public Safety Answering Points (PSAPs), Interactive Media Response (IMR) FEs, bridges and other elements that terminate calls from entities outside an ESInet that may be behind NATs must implement “Interactive Connectivity Establishment (ICE)”, RFC 8445 [5] which includes support for “Session Traversal Utilities for NAT (STUN), RFC 5389 [6]. ESInets/NGCS SHOULD maintain a “Traversal Using Relays around NAT (TURN)” (RFC 5766) [7] server for use by entities inside the ESInet placing outbound calls.

2.2 Interconnect Availability
NENA-STA-010 prescribes multiple interconnected private, managed and routed ESInets. Interconnection enables every ESInet the ability to route traffic to any point in any other ESInet. A large region, state or province could implement a backbone ESInet connecting to every PSAP or to all the smaller regional ESInets. Neighboring states or provinces, entire
countries, and ultimately the world can all interconnect their ESIInets, thus producing the highest level of availability. Figure 1 below depicts potential interconnection points in a transitional network environment in which information is received from both legacy and NG9-1-1 sources for dissemination to first responders over both legacy and IP-based network availability.

ESIInets currently are primarily at the state and/or regional level, and peer with one another. PSBNs SHOULD peer with state or regional ESIInets. For routing of messages to be optimal, and for the interconnections to be efficient, with proper reliability, availability, and survivability, it is important for PSBNs and ESIInets to peer. Peering also enhances interoperability between responders and agencies in large-scale incidents where bandwidth requirements can increase substantially. With a PSBN and ESIInet connected as peers in a high-availability configuration, larger amounts of bandwidth may be available to agencies for large incidents. There is a cost factor for each interconnection and for the peak bandwidth that must be supported to handle large incidents. Connecting a PSBN directly to every PSAP can provide sufficient availability, but at a cost. Connecting at the ESIInet and at every PSAP provides more redundancy, but again at a cost. If not doing both, peering is a better choice from the availability per cost perspective. In addition, smaller PSAPs may
not have the personnel resources necessary to manage availability on their side of the interconnect. Because lack of bandwidth affects availability, the interconnect MUST provide sufficient bandwidth to support the largest-scale incident expected in the area covered by the interconnect. Figure 2 below depicts an end-state (all-IP) network environment in which all incoming and outgoing data sources are IP-based, and all legacy elements have been retired.

Figure 2 End-State ESInet-PSBN Network Environment

NENA-INF-016, Emergency Services IP Network Design Information Document [37], provides information on bandwidth requirements for handling emergency calls but does not cover bandwidth requirements for exchanging data with responders. The responder data can be significant because it can include video and images sent in either direction. ESInet and PSBN interconnect architects MUST consider the type and volume of data that will be exchanged, with expected growth, and provide sufficient bandwidth to support it. Figure 3 below depicts redundant network elements at Layer 1 of the OSI model. Geographically diverse fiber links, preferably from different fiber providers, point-to-point microwave links, and satellite connections are all viable means of creating the redundancy and resiliency at the physical layer of the network.
2.2.1 Redundant Geo-diverse Connections

Satellite networks are a non-terrestrial diversity option cited as an FCC Communications Security, Reliability and Interoperability Council (CSRIC) Best Practice BP Number 12-9-3238 [42] for Public Safety to use to transport NG9-1-1 when terrestrial networks are disrupted or not available. Non-terrestrial Multiprotocol Label Switching (MPLS) via satellite may support interconnection diversity but legacy satellite facilities may not provide the same performance capabilities.

2.2.2 Physical Diversity

In order to be fully independent and physically diverse, the links must not share any components in common (i.e., not in the same trench, not running through the same Digital Cross Connect at the Central Office, routers not from the same vendor, etc.) As depicted in the diagram above, physical diversity also includes Open Systems Interconnection (OSI) Layer diversity (different types of physical wired and wireless interconnections).
2.2.3 Provider Diversity

Using links from different providers reduces the chance that a failure in a single provider’s facilities, equipment, or services can interrupt service. This is also true for the equipment used by multiple providers. For example, using routers from the same vendor on all paths can make service vulnerable to problems unique to that vendor’s equipment.

All data circuits (interconnections) and network components which comprise an ESInet SHOULD be monitored with notifications sent to an approved management system. All operational network components that form an ESInet and network management systems SHOULD support the Network Configuration Protocol (NETCONF) per RFC 6241 [8]. Components and management systems on the ESInet side of the interconnect MUST support Transport Layer Security (TLS) with Mutual X.509 Authentication per RFC 7589 [9] and SHOULD support subscribing and receiving asynchronous event notifications as specified in RFC 5277 [10]. Network components and management systems SHOULD also support monitoring the NETCONF protocol as defined in RFC 6022 [11]. Additional information about monitoring and managing NG9-1-1 networks, elements, and services can be found in NENA-INF-016 Emergency Services IP Network Design [37]. and NENA-INF-040 Monitoring and Managing NG9-1-1 [38].

2.2.4 Failure Mitigation

FCC CSRIC Best Practice number 12-10-5261 [43] advises network operators, service providers, public safety and property managers to identify interconnection points and coordinate restoral plans. Plans SHOULD be detailed in negotiated Service Level Agreements (SLAs) between stakeholders. A good high-availability design is critical to surviving a failure of one portion of the service infrastructure. Having written processes and procedures for restoring service on that portion of the infrastructure is critical to restoring high availability. SLAs SHOULD clearly identify demarcation points between responsible parties and define the process of identifying and correcting problems with clearly defined responsibilities. NENA-INF-016 Emergency Services IP Network Design [37] provides details on SLAs between parties on ESInets. Appropriate SLAs MUST exist between ESInet and PSBN operators.

2.3 Identity, Authentication, and Access

2.3.1 Identity

NENA’s i3 Architecture [53] has a uniform notion of identity. Each agency is identified by an “AgencyID” which is a DNS domain name, like psap.allegheny.pa.us. Each agent (person or automaton) is identified by an “AgentID” which is in an agent@agency form, like bill.smith@psap.allegheny.pa.us. Each agency and each agent has a set of “credentials” which are public and private key pairs using public key cryptography. The i3
Architecture defines Element Identifiers for devices, which have their own credentials, but almost all transactions use the Agent or Agency identifiers for authorization. If different identifiers will be used on the ESInet and PSBN to identify the same user, then a mapping mechanism will be required, and will be defined in future work. The i3 Architecture defines a set of Roles that can be assigned to entities in the ESInet. Future work will define required mapping between i3 Roles and those used in PSBNs.

The credentials in NG9-1-1 are created within a “Public Key Infrastructure” (PKI) that has a root of trust called the PSAP Credentialing Agency (PCA) [41]. The public key for each agency and each agent is represented by an x.509 certificate, which is signed by a Certificate Authority (CA). The public key of the CA is signed by another CA, and there can be a tree of CAs that have a root CA, which is the PCA. Typically, there is a State CA, which has its key signed by the PCA, and there is a regional or local CA whose key is signed by the State CA. Typically agency certs for PSAPs are signed by the State CA, and agent certs are signed by a local CA. All entities in NG9-1-1 require credentials signed by a CA whose cert is “traceable” to the PCA.

Some kinds of agencies might not accept the PCA as their trust root. To achieve common trust among all the agencies, the certs of the root CAs cross sign, either with each other, or preferably through the “Federal Bridge Certification Authority” (FBCA) [44] which is a CA established to do precisely that: federate trust by cross signing root CA certificates. Each root CA has its certificate cross signed by the FBCA and then trust can be established between entities in different PKIs.

Responder networks might have no common notion of identity, and no common notion of credentials. Accordingly, adoption of the NENA i3 Architecture identity and credentialing scheme, with multiple, federated PKIs is needed.

All agencies and agents wishing to communicate SHALL be identified by agencyIDs and agentIDs as defined in NENA-STA-010 [53]. While device Element Identifiers MAY be used in certain circumstances, most communications SHOULD use the Agency or Agent identifier to determine authorization.

Every agent and every agency SHALL obtain credentials traceable to the PCA or other root Certificate Authority designated by the appropriate agency type organization (International Association of Chiefs of Police, National Fire Protection Association, etc.). Each root CA’s cert SHALL be cross signed by the Federal Bridge CA.

Each Functional Element (FE) (or group of FEs, if a single implementation has multiple FEs) SHALL be identified by an ElementId as defined in STA-010, and SHALL have credentials traceable to the appropriate root CA.

All FEs, applications and services SHALL use element, agent, and agency identifiers in the form defined in STA-010 exclusively to identify FEs, agents and agencies in all exchanges.
of data. Whether the responder is an individual agent or a unit of some type, it is typically
the responder device that reports status, such as location or device state. Responder
devices SHALL use identifiers similar to Element Identifiers as defined in STA-010 – a fully
qualified hostname and have credentials traceable to the PCA that are used to authenticate
the device.

It is essential that when responding to an incident, whether a single or multi-agency
incident, that all applications have a common notion of identifiers. Accordingly, the Incident
Identifier, and where needed, the Call Identifier from NENA-STA-010 SHALL be used in all
communication between entities across an ESInet and a PSBN where a specific incident, or
a specific 9-1-1 call respectively is identified.

2.3.2 Data Rights Management
Agencies need the ability to control who has access to their data, regardless of the
applications, networks or protocols that are used to access the data. This is called “Data
Rights Management” (DRM). The owner of the data is the entity that created it. NG9-1-1
has standardized how Data Rights Management is mechanized. The owner’s decisions on
who can do what with specific data is expressed in a “Policy”. The Policy language is
standardized, using eXtensible Access Control Markup Language (XACML) [47]. The Policy
is stored in a Policy Store, which has a standardized interface to read and write policies. All
protocol interactions between entities within or between ESInets enforce the policy. The
object of a policy is a specific piece of data, such as an Emergency Incident Data Object
(EIDO), and the actors in the policy are agents, agencies, devices and automatons. The
policies grant read, write and/or delete access to the data object or portions of the data
object. Policies are stored in the Policy Store under the agency that owns the data, and the
name of the policy, which is standardized for a specific kind of data. NG9-1-1 allows a
Policy Store to be co-located with any FE, but the standards require that all FEs be able to
be provisioned with the policy store that will be used. Policies may be replicated between
policy stores so that redundancy and efficient access can be achieved.

Because there is no known equivalent of this Data Rights Management mechanism in any
PSBN, the Data Rights Management system standardized in NG9-1-1 and defined in NENA-
STA-010 [53] MUST be used in all transactions between an ESInet and a PSBN. Any
development work that maps between different DRM mechanisms will be described in
future work.

2.4 Privacy and Integrity Protection
In every instance where two entities exchange data across the ESInet and PSBNs, the
protocol exchanges MUST be protected by Transport Layer Security (TLS). TLS 1.2 (see
RFC 5246 [12]) MUST be supported by all entities. TLS 1.3 (see RFC 8446 [13]) SHOULD
be supported by all entities unless they were in service prior to this standard being
released. TLS MUST use mutual authentication. Implementations MUST NOT offer or accept TLS 1.1 or TLS 1.0. Perfect Forward Secrecy MUST be used within the ESInet and/or the PSBN.

Credentials used MUST be traceable to the PCA or other root CA cross signed with the PCA (see Section 2.3.1 of this document). Entities MUST accept credentials traceable to the PCA or other cross signed root CAs although policy SHALL govern which entities are allowed to connect and transfer data.

All implementations MUST support RSA-2048 (see RFC 8017 [14]). RSA-1024 (see RFC 3447 [15]) MAY be supported. Authentication algorithms stronger than or equivalent to RSA-2048 MAY be supported in addition to RSA-2048.

All implementations MUST support SHA-256 (see FIPS-PUB-180-4 [45]). SHA-1, SHA-2 or MD5 MUST NOT be allowed. Integrity protection algorithms stronger than or equivalent to SHA-256 MAY be supported in addition to SHA-256.

All implementations MUST support AES-256 (see FIPS-PUB-197 [46]). AES key strengths less than 256 bits MUST NOT be allowed. Encryption algorithms stronger than, or equivalent to AES-256 may be supported in addition to AES-256.

Where SIP protocol exchanges are performed, they MUST be protected with TLS using the above minimum requirements.

Where real time media is sent across the ESInet/PSBN boundary, the media MUST be protected with DTLS-SRTP using the above minimum cipher requirements (see RFC 5763 [16] and RFC 5764 [17]).

Cryptology choices are constantly being re-evaluated due to ongoing threat analysis, algorithm weakness research and other factors. Implementers should be aware that the mandatory algorithm choices (RSA-2048, SHA-256, and AES-256) to be supported in all implementations as described in this section may need to be upgraded as new threats emerge. At present, only a future revision of NENA-STA-010 [53] could change the mandatory algorithm requirements.

### 2.5 Digital Signatures

Digital Signatures provide two benefits: 1) verification that the data that was received has not been modified from when it was signed, and 2) verification of the signer’s identity (non-repudiation). As in NENA-STA-010.3 (forthcoming), specific Services, including the Logging Service and the Policy Store, support the implementation of JSON Web Signature specification (JWS) (NENA-STA-010.3, JSON Web Signatures) digital signatures. The JWS approach defines a standard way to apply digital signatures to JSON data structures based on X.509 certificates for authentication, authorization, and non-repudiation between any two entities. Signing is done using the private key of the signing entity which is traceable.
to the PCA after which the recipient can then authenticate using the that same signer’s public key.

PSBN elements that use the Services from STA-010 that support digital signatures, or that need digital signatures for other reasons, SHALL use JWS as specified in NENA-STA-010.3.

2.5.1 Data Alteration Protection
Digital signatures for JSON objects using JWS rely on the Public/Private Key pair to create a digital hash of the JSON object to ensure that the data object has not been tampered with after it was originally signed as it is exchanged between or across networks. The signing process by the originating entity is repeated by the receiving entity to determine if the hash value is the same. If it is the same, the JSON object received is proven to be the same as that which was sent.

2.6 Data and Media Interoperability
The ESInet-PSBN interconnection MUST support passing interactive and non-interactive media and data between Responders and PSAPs. In NG9-1-1, SIP is used for emergency calls, with interactive voice, video, and text media. Non-interactive media may be included in any call. Incident data is exchanged in JavaScript Object Notation (JSON, RFC 8259 [18]) formatted as Emergency Incident Data Objects (EIDOs, NENA-STA-021 [39]). Details on Data Rights Management in NG9-1-1 are provided in Section 2.3.2 of this document.

2.6.1 Call Media
It may be necessary to connect a Responder to an emergency or non-emergency call. Media in NG9-1-1 calls are delivered via the Real-Time Protocol (RTP) RFC 3550 [19]. Media are negotiated between endpoints using the Session Description Protocol (SDP) RFC 4566 [20] and media is identified with media labels. Media streams for voice, video, and text are carried on RTP over User Datagram Protocol (UDP) in the ESInet, preferably employing media security with Secure Real-Time Protocol (SRTP) using Datagram Transport Layer Security (DTLS) as specified in RFC 5763 [21] and RFC 5764 [22]. Real-Time Control Protocol (RTCP) as defined in RFC 3550 [19] and Secure Real-Time Control Protocol (SRTCP) as defined in RFC 5764 [21] are used within the ESInet whenever possible. PSAP User Agents support RTCP Extended Reports (RTCP XR, RFC 3611) [23]. Responder User Agents SHOULD support RTCP XR.

In order to ensure that calls can be transferred to or conferenced with Responder devices, the ESInet-PSBN interconnection MUST allow the protocols and media described in this section to operate properly across the interconnect boundary. Transfers and conferencing are accomplished as specified in NENA-STA-010 [53]. Network architects MUST consider the implication of Network Address Translation and differing security mechanisms at the
interconnect boundary to ensure that traffic is not hampered, and proper security can be maintained on both sides of the interconnect. See Section 2.1.2 and Section 2.4 for details.

2.6.1.1 Voice Call Media

Media in voice calls typically use G.711 compression with μ-law or A-law companding (the latter is to support devices intended for use in other parts of the world). Voice media MAY use other CODECs, including EVS, AMR, AMR-WB, G.722, G.729A/B, and OPUS.

2.6.1.2 Video Call Media

Video media in NG9-1-1 calls is typically H.264/MPEG-4 Version 10, with a minimum baseline support for levels 1 through 3. User Agents in the ESInet/NGCS support both RFC 5104 [24] and RFC 5168 [25] for full frame refresh requests. To maintain the ability to support rapid fingerspelling for sign language users, ESInet/NGCS elements attempt to maintain at least 30 frames per second video if offered by the sender. RTP with Audio-Visual Profile Feedback (AVPF) (RFC 4585 [26]) is supported in the ESInet/NGCS and is preferred in offers.

2.6.1.3 Real-Time Text (RTT)

All call handling elements in the ESInet/NGCS support RTP Payload for Text Conversation (RFC 4103 [27]). All call handling elements except the LNG and LPG MUST also support the update for multi-party real-time text calls defined in RTP-mixer formatting of multi-party Real-time text (forthcoming, [28]). Information on application of real-time text can be found in Framework for Real-Time Text over IP Using the Session Initiation Protocol (SIP) (RFC 5194 [28]).

2.6.1.4 Instant Messaging

MSRP is used in NG9-1-1 for instant message communications between persons, including messages that were sent to 9-1-1 as SMS text messages.

2.6.1.5 Non-interactive Calls

Per NENA-STA-010 [53], non-interactive calls, also called data-only emergency calls, are emergency calls that are initiated automatically, carry data, are not necessarily associated with a person, and do not establish two-way interactive media sessions. Non-interactive calls presented to an ESInet are signaled with a SIP MESSAGE method request. These calls are typically directed to a PSAP but may be forwarded to a Responder by copying the content and sending it in a new MESSAGE request.

Advanced Automatic Crash Notification (AACN) calls can establish interactive media and are associated with a human vehicle occupant. A non-interactive call from a vehicle might be placed by an element that is not designed to communicate with vehicle occupants (e.g., a
sensor module embedded in the vehicle without speaker or microphone access) and does not provide interactive two-way media. Such non-interactive calls are delivered via SIP MESSAGE method. An associated voice or video call would use the methods described in NENA-STA-010 for those call types. Interactive and non-interactive calls associated with an Advanced Automatic Crash Notification system may be forwarded to a Responder.

2.6.2 Responder Data Services (RDS)
Responders in the field need reliable network paths for sharing real-time data related to an Incident. The forthcoming NG9-1-1 PSAP Standard, NENA STA-023 [40], defines the RDS FE for this purpose. The RDS FE has an interface on the agency side (RdsPsap) and one on the responder side (RdsResponder) and uses the Emergency Incident Data Object (EIDO) as the primary method of exchanging data. Access to data in NG9-1-1 is described in Section 2.3.2 of this document.

Protocols for exchanging EIDOs between FEs are defined in NENA-STA-024, the NENA/APCO Standard for the Conveyance of Emergency Incident Data Objects between NG9-1-1 Systems and Applications [39] (forthcoming). The RDS supports location updates via SIP SUBSCRIBE/NOTIFY (RFC 6665 [29]) and HELD (HTTP Enabled Location Delivery, RFC 5985 [30]). Accordingly, the ESInet-PSBN interface MUST support exchange of data between responders and agencies via SIP SUBSCRIBE/NOTIFY and HTTP. A gateway with an RDS interface may be used if needed to support responder devices and applications that don’t support the RdsResponder interface directly.

EIDOs may contain links to streaming media sources that provide one-way, non-interactive media (text, audio, video) in the form of a Real-Time Streaming Protocol (RTSP 2.0 [31]) URL.

2.6.3 Media Proxy
One-way non-interactive media may be streamed to or from Responders. An example would be video from a surveillance camera streamed to a Responder. Media from a Responder’s body-worn or vehicle-mounted camera would typically be streamed to the Agency. NENA’s NG9-1-1 PSAP Standard, NENA-STA-023 (forthcoming) [40], defines a Media Proxy FE that forwards streaming media to and accepts streaming media from a Responder while ensuring that the media and associated metadata are logged. The Real-Time Streaming Protocol (RTSP 2.0 [31]) is used for streaming media between a Responder and the Media Proxy FE.

The Media Proxy FE accepts a URI from a streaming media source and provides a local URI to allow access to that media source through the Media Proxy FE. The viewer/listener accesses the stream through the Media Proxy FE’s local URI so that the Media Proxy FE can ensure that the media and metadata being sent to the viewer/listener is logged.
The Media Proxy FE enforces policy of the Agency controlling which Agents/Responders are allowed access to what media.

Access to one-way non-interactive streaming MUST be done through the Media Proxy FE. All implementations must support authorization of users’ access to media streams according to the policy of the owning Agency.

All implementations that interface to the Media Proxy FE MUST support RFC 7826 *Real-Time Streaming Protocol Version 2.0* [31] for streaming media sources and viewers/listeners. A gateway may be used to support legacy RTSP 1.0 applications, but such implementations are not standardized. The Media Proxy FE MAY support other protocols, but none are standardized at this time.

All implementations MUST support carrying multiple output streams that originated from a single input stream, so that multiple users can view/listen to the same stream simultaneously.

**2.6.4 Multicast Video Support**

Supporting IP Multicast presents some challenges when the client is on a different network, but the benefits of IP Multicast can be significant. Agencies can use it to cast video briefings or feeds from surveillance cameras to responders via their vehicle or handheld devices. Multicast requires less bandwidth on the source network, and the benefit can be significant when sending data to a larger number of clients. The network interconnect SHOULD allow Multicast traffic, if possible, in cases where the destination network supports Multicast. Multicast may become more common in the future on PSBNs due to its benefits, but it must be supported on both networks to function. The interconnect architect SHOULD plan for this future possibility and not preclude it.

**2.7 Peering Issues**

**2.7.1 Network-to-Network Interface (NNI)**

Network-to-Network Interfaces connect two disparate networks. One common example is the connection from one internet service provider (ISP) to another ISP. The Border Gateway Protocol (BGP) provides for the exchange of routing information between the two networks. Another example is the NNI between two Voice over Internet Protocol (VoIP) providers. In either case, one provider orders point-to-point connectivity to the other provider provisioned for sufficient bandwidth for the expected traffic load. The physical interconnection may take place at a router or firewall device, or in the case of VoIP traffic, at a session border controller.

The management of the connection is based on mutual trust between the two service providers. Security measures include but are not limited to, Border Gateway Protocol (BGP,
RFC 4271 [32]) authentication, session border controllers, firewalls, virtual private network connections, and virtual routing and forwarding instances.

2.7.2 Maintaining Quality of Service (QoS) Across the NNI

Quality of Service (QoS) provides a means of managing traffic flows in a network and giving priority to critical traffic to ensure that it is transported and delivered in a timely manner. The protocol implemented to accomplish this is the Differentiated Services Code Point (DSCP) protocol as defined in IETF RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers* [33]. Generally, service providers do not honor the DSCP field from other providers. In the case of a private NNI, such as would be implemented for public safety, the providers must agree to honor the per-hop behaviors which may require mapping between the DSCPs of the two networks.

The ESInet requires the use of DiffServ (RFC 2474 [33] and RFC 2475 [35]) and specifies DSCPs that mark specific traffic types (e.g., emergency call SIP messages, audio media packets, video media packets) as well as suggested Per Hop Behaviors (PHBs) for those traffic classes. Many PSBNs serve a wider range of customers than ESInets do, and the number of traffic types they serve greatly exceeds the DSCP code space. Accordingly, the PSBNs commonly use DSCP code points that directly map to specific PHBs defined in RFC 2597 [48], with RFC 3246 [49], and RFC 3247 [50]. Mappings from ESInet DSCP markings to PSBN DSCP markings could be specified as long as there are equivalent PHBs: the mapping would map the ESInet traffic type to the PSBN’s PHB marking that the ESInet provided to that traffic type. Mapping the other way cannot be made precise, because the information on what the PSBN traffic type is cannot be inferred by the edge router — it is lost between the device that knows what the traffic is, the PSBN network that can’t convey that information, and the ESInet default behavior has more than one traffic type with the same PHBs. Nevertheless, a choice can be made when traffic arrives at the edge router of which class to mark the traffic as, and at least the right PHBs can be maintained. Either network can provide the mapping, or each network can mark traffic entering its network. All routers SHOULD implement DiffServ and respect codepoints, or at least be transparent to the markings.

The mechanisms used for traffic priority and marking in PSBNs is not well known. The mechanisms used on the ESInet are well-defined. NENA assumes that there will be differences in DSCPs used for traffic marking. It is critical that a network interconnection agreement between the ESInet and PSBN provider ensures that priority is maintained as much as possible from end to end across both networks. Mapping of DSCPs between the networks SHOULD be specified in the SLA between the two network providers.

Quality of Service (QoS) provides a means to manage different priorities and performance guarantees for applications and protocols traversing a network. QoS is NOT a substitute for
bandwidth, nor does it create bandwidth. Proper bandwidth capacity planning for the contiguous IP path that requires QoS is critical for QoS to be effective. That IP path, in many cases, spans across multiple provider networks. There is a cost for bandwidth, so it is never unlimited. QoS becomes particularly critical in circumstances where the network is impaired, and bandwidth is less available. It is therefore important that QoS is handled as optimally as possible across the ESInet-PSBN boundary.

DiffServ-based QoS consist of 3 main components: Defining “Service Classes”, “Marking” traffic with DSCP values associated to the service classes, and Defining “Per Hop Behavior” (scheduling, queuing, policing, or shaping) for the service classes. Together these 3 components define a QoS strategy. Each PSBN service provider typically will have their own QoS strategy that aligns with the overall purpose and requirements of their network. ESInets have a common QoS strategy that will differ from a given PSBN. Therefore, it is critical that a network interconnection agreement between the PSBN and ESInet providers defines the required priority and performance for the relevant applications and protocols so that performance SLAs can be maintained end-to-end across both networks, with support for the respective QoS strategies.

The nature of the NNI between an ESInet and a PSBN requires that the two networks recognize the markings of the traffic being exchanged and map those markings to their appropriate markings per a Service Level Agreement (SLA) between the two network operators. The SLA SHOULD be re-evaluated, and mappings confirmed at least once per year so that changes in markings or technology on one side don’t invalidate the effectiveness of the QoS strategy.

Applications on the PSBN that communicate with entities on the ESInet should mark traffic per the SLA between the two network providers so that the traffic will receive the desired treatment on the ESInet. Applications that are intended to run on multiple PSBNs SHOULD mark traffic per the SLA for that PSBN because traffic marked incorrectly might get incorrect treatment on the ESInet of the destination agency, and critical traffic could be dropped. Proper marking on the PSBN ensures proper treatment on all ESInets.

NOTE: Guidelines for the ESInet QoS strategy and any influence of definition related to the PSBN QoS strategy, should be generally aligned with the specifications in the following IETF RFCs:

- IETF RFC 2474 Definition of the Differentiated Services Field [33]
- IETF RFC 2475 Architecture for Differentiated Services [35]
- IETF RFC 2597 Assured Forwarding PHB Group [48]
- IETF RFC 3246 An Expedited Forwarding PHB (Per-Hop Behavior) [49]
- IETF RFC 3247 Supplemental Information for the New Definition of the EF PHB [50]
- IETF RFC 3260 New Terminology and Clarifications for Diffserv [51]
2.8 Logging and Chain of Custody

NENA-STA-010 [53] defines a Logging Service for logging and recording emergency call and incident media and data. Data exchanged with responders is logged by the agency Functional Elements (FEs), typically Responder Data Services and Media Proxy, that send and receive the data to create a legal record of an agency’s involvement in an incident and maintain a record of the “chain of custody” of the logged information from the time it was first captured. The Logging Service has four interfaces:

1. A web service interface for logging structured event data in JSON and XML format
2. A web service interface for retrieving logged JSON/XML data
3. A SIPREC (SIP REcording) interface for recording streaming media
4. An RTSP 1.0\(^1\) or 2.0 interface for playing back recorded streaming media

The web services are REST/JSON (the JSON data may contain XML as HTTP-encoded text).

Data shared directly between responders in the field without going through an agency FE will not be captured unless the applications sharing the data log it themselves. Devices and applications that share data directly between responders SHOULD log the data to the Logging Service to create a legal record of the exchange and to allow a chain of custody to be established.

The ESInet-PSBN interconnect MUST allow responder devices and applications to log data to the Logging Service across the interconnect boundary, either directly or through Responder Data Services and/or Media Proxy and SHOULD NOT preclude the device or application from logging to at least two Logging Services simultaneously for redundancy.

3 NENA Registry System (NRS) Considerations

Not Applicable.

4 Documentation Required for the Development of a NENA XML Schema

Not Applicable.

5 Impacts, Considerations, Abbreviations, Terms, and Definitions

5.1 Operations Impacts Summary

Maintaining network infrastructure to support a negotiated SLA with another connected network requires management resources.

---

\(^1\) Logging Services implemented prior to earlier versions of NENA-STA-010 may have RTSP 1.0 interfaces. NENA-STA-010.3 mandates RTSP 2.0.
5.2 Technical Impacts Summary
Properly implemented, the standards and recommendations included in this document will enhance interoperability across key sectors of the public safety ecosystem. In particular, data and information sharing between the general public requesting emergency services, the PSAP answering their initial requests, and the first responders dispatched to address the emergency will be enabled and enhanced by implementing this standard. ESInet to PSBN interconnection and interoperability is needed to enable the promise of NG9-1-1 and NG public safety in general, so proper implementation of this standard will have significant technical impact on the implementation of NG9-1-1.

5.3 Security Impacts Summary
The security requirements detailed in this document will directly impact security configuration on both sides of the NNI.

5.4 Recommendation for Additional Development Work
If different identifiers or roles will be used on the ESInet and PSBN to identify the same entity, then a mapping mechanism will be defined in future work.

Future work may define a mapping between the DRM mechanisms used in the ESInet and the DRM mechanisms used in the PSBN where required.

5.5 Anticipated Timeline
This standard may be implemented immediately upon publication. Doing so will facilitate interoperability as agencies migrate to full NG9-1-1 functionality.

5.6 Cost Factors
With a PSBN and ESInet connected as peers in a high availability configuration, larger amounts of bandwidth may be available to agencies for large incidents. There is a cost factor for each interconnection and for the peak bandwidth that must be supported to handle large incidents. Connecting a PSBN directly to every PSAP can provide sufficient availability, but at a cost. Connecting at the ESInet and at every PSAP provides more redundancy, but again at a cost. If not doing both, peering is a better choice from a cost perspective.

5.7 Cost Recovery Considerations
The authors of this document are unaware if there are, or may be in the future, grants or other funding programs that would cover costs for interconnecting ESInets and PSBNs and managing the interconnections.
5.8 Additional Impacts (non-cost related)

The specifications and recommendations in this NENA document are designed to increase interoperability between interconnected ESInets and PSBNs and between applications and devices that communicate across the interconnection. Implementations based on this document are expected to provide the high degree of interoperability required to support the rich applications required in NG9-1-1.

5.9 Abbreviations, Terms, and Definitions

See NENA Master Glossary of 9-1-1 Terminology, NENA-ADM-000 [1], for a complete listing of terms used in NENA documents. All abbreviations used in this document are listed below, along with any new or updated terms and definitions.

<table>
<thead>
<tr>
<th>Term or Abbreviation (Expansion)</th>
<th>Definition / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9-1-1 Authority</td>
<td>A State, County, Regional or other governmental entity responsible for 9-1-1 service operations. For example, this could be a county/parish or other local government, a special 9-1-1 or Emergency Communications District, a Council of Governments or other similar body.</td>
</tr>
<tr>
<td>CA (Certificate Authority)</td>
<td>A trusted entity that issues digital certificates. The Certificate Authority conducts a vetting process to ensure that the holder of the digital certificate is who they claim to be. Digital certificates are an essential part of secure communication and play an important part in the PKI (Public Key Infrastructure).</td>
</tr>
<tr>
<td>CSRIC (Communications Security, Reliability and Interoperability Council)</td>
<td>An advisory body of the FCC, formerly known as NRIC (Network Reliability and Interoperability Council), which provides recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media, and public safety.</td>
</tr>
<tr>
<td>DHCP (Dynamic Host Control Protocol (i2); Dynamic Host Configuration Protocol)</td>
<td>A widely used configuration protocol that allows a host to acquire configuration information from a visited network and, in particular, an IP address.</td>
</tr>
<tr>
<td>DNS (Domain Name System)</td>
<td>A globally distributed database for the resolution of host names to numeric IP addresses.</td>
</tr>
<tr>
<td><strong>DRM (Data Rights Management)</strong></td>
<td>As used in this document, Data Rights Management refers to a set of technologies used to protect sensitive information from unauthorized access.</td>
</tr>
<tr>
<td><strong>EIDO (Emergency Incident Data Object)</strong></td>
<td>A JSON-based (JavaScript Object Notation) object that is used to share emergency incident information between and among authorized entities and systems. NENA has adopted the JSON-based EIDO (Emergency Incident Data Object) for sharing incident information among authorized NG9-1-1 entities and systems.</td>
</tr>
<tr>
<td><strong>ESInet (Emergency Services IP Network)</strong></td>
<td>An ESInet is a managed IP network that is used for emergency services communications, and which can be shared by all public safety agencies. It provides the IP transport infrastructure upon which independent application platforms and core services can be deployed, including, but not restricted to, those necessary for providing NG9-1-1 services. ESInets may be constructed from a mix of dedicated and shared facilities. ESInets may be interconnected at local, regional, state, federal, national, and international levels to form an IP-based inter-network (network of networks). The term ESInet designates the network, not the services that ride on the network. See NG9-1-1 Core Services.</td>
</tr>
<tr>
<td><strong>FBCA (Federal Bridge Certification Authority)</strong></td>
<td>A PKI (Public Key Infrastructure) Bridge or link between the Federal Common Policy Certification Authority and other CAs that comprise the Federal PKI network and that may operate under comparable but different certificate policies.</td>
</tr>
<tr>
<td><strong>FE (Functional Element)</strong></td>
<td>An abstract building block that consists of a set of interfaces and operations on those interfaces to accomplish a task. Mapping between functional elements and physical implementations may be one-to-one, one-to-many or many-to-one.</td>
</tr>
<tr>
<td><strong>ICE (Interactive Connectivity Establishment)</strong></td>
<td>A mechanism for endpoints to establish RTP connectivity in the presence of NATs and other middle boxes.</td>
</tr>
<tr>
<td><strong>IMR (Interactive Media Response)</strong></td>
<td>An automated service used to play announcements, record responses, and interact with callers using any or all of audio, video, and text.</td>
</tr>
<tr>
<td><strong>MPLS (Multi-Protocol Label Switching)</strong></td>
<td>A type of data-carrying technique for high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. A mechanism that allows network administrators to perform a measure of traffic engineering within their networks.</td>
</tr>
<tr>
<td><strong>NAT (Network Address Translation)</strong></td>
<td>Maps a single public address to one or many internal addresses and all network IP addresses on the connected computers are local and cannot be seen by the outside world.</td>
</tr>
<tr>
<td><strong>NENA (National Emergency Number Association)</strong></td>
<td>The National Emergency Number Association is a not-for-profit corporation established in 1982 to further the goal of “One Nation-One Number.” NENA is a networking source and promotes research, planning, and training. NENA strives to educate, set standards, and provide certification programs, legislative representation, and technical assistance for implementing and managing 9-1-1 systems. <a href="http://www.nena.org">www.nena.org</a></td>
</tr>
<tr>
<td><strong>NETCONF (Network Configuration Protocol)</strong></td>
<td>A protocol that provides mechanisms to install, manipulate, and delete the configuration of network devices.</td>
</tr>
<tr>
<td><strong>NGCS (Next Generation 9-1-1 Core Services)</strong></td>
<td>The base set of services needed to process a 9-1-1 call on an ESInet. Includes the ESRP, ECRF, LVF, BCF, Bridge, Policy Store, Logging Services and typical IP services such as DNS and DHCP. The term NG9-1-1 Core Services includes the services and not the network on which they operate.</td>
</tr>
<tr>
<td><strong>NGCS (Next Generation 9-1-1 [NG9-1-1] Core Services)</strong></td>
<td>The base set of services needed to process a 9-1-1 call on an ESInet. Includes the ESRP, ECRF, LVF, BCF, Bridge, Policy Store, Logging Services, and typical IP services such as DNS and DHCP. The term NG9-1-1 Core Services includes the services and not the network on which they operate. See Emergency Services IP Network</td>
</tr>
<tr>
<td><strong>NNI (Network-to-Network Interface)</strong></td>
<td>An interface that specifies signaling and management functions between two networks.</td>
</tr>
</tbody>
</table>
| OSI (Open Systems Interconnection) | A 7-layer hierarchical reference model structure developed by the International Standards Organization for defining, specifying, and relating communications protocols; not a standard or a protocol. Layer Description  
(7) Application: Provides interface with network users  
(6) Presentation: Performs format and code conversion  
(5) Session: Manages connections for application programs  
(4) Transport: Ensures end-to-end delivery  
(3) Network: Handles network addressing and routing  
(2) Data Link: Performs local addressing and error detection  
(1) Physical: Includes physical signaling and interfaces |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PCA (PSAP Credentialing Agency)</td>
<td>The root authority designated to issue and revoke security credentials (in the form of an X.509 certificate) to authorized 9-1-1 agencies in an i3-compliant infrastructure.</td>
</tr>
<tr>
<td>PKI (Public Key Infrastructure)</td>
<td>A set of hardware, software, people, policies, and procedures defined in a Certificate Policy to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.</td>
</tr>
<tr>
<td>Policy Store</td>
<td>A functional element in the ESInet that stores policy documents/rules.</td>
</tr>
<tr>
<td>PSAP (Public Safety Answering Point)</td>
<td>A physical location where 9-1-1 emergency telephone calls are delivered to and answered for a defined geographic service area.</td>
</tr>
<tr>
<td>PSBN (Public Safety Broadband Network)</td>
<td>An interoperable broadband communications network used by emergency responders to communicate with each other and acquire and share information during emergencies, planned events, and day-to-day events. The PSBN is designed to deliver mission-critical services to public safety users.</td>
</tr>
<tr>
<td>SIP (Session Initiation Protocol)</td>
<td>A protocol specified by the IETF (RFC 3261) that defines a method for establishing multimedia sessions over the Internet. Used as the call signaling protocol in VoIP, NENA i2, and NENA i3.</td>
</tr>
<tr>
<td>SLA (Service Level Agreement)</td>
<td>A service level agreement is a contract between a service provider (either internal or external) and the end user that defines the level of service expected from the service provider. SLAs are output-based in that their purpose is specifically to define what the customer will receive.</td>
</tr>
<tr>
<td>Protocol/Standard</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>STUN (Session Traversal Utilities for NAT)</td>
<td>A protocol that serves as a tool for other protocols in dealing with Network Address Translator (NAT) traversal.</td>
</tr>
<tr>
<td>TLS (Transport Layer Security)</td>
<td>An Internet protocol that operates between the IP layer and TCP and provides hop-by-hop authentication, integrity, protection, and privacy using a negotiated cipher-suite.</td>
</tr>
<tr>
<td>TURN (Traversal Using Relays Around NAT)</td>
<td>A mechanism for establishing RTP connections through some kinds of NAT devices that won’t allow two endpoints to connect directly. TURN uses a relay outside the NAT boundaries.</td>
</tr>
<tr>
<td>UA (User Agent)</td>
<td>As defined for SIP in IETF RFC 3261 [3], the User Agent represents an endpoint in the IP domain, a logical entity that can act as both a user agent client that sends requests, and as user agent server responding to requests.</td>
</tr>
<tr>
<td>X.509</td>
<td>An ITU-T standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI). In NG9-1-1, refers to the format of a certificate containing a public key.</td>
</tr>
<tr>
<td>XACML (eXtensible Access Control Markup Language)</td>
<td>A general-purpose access control policy language that provides an XML-based syntax for defining rules to control access to resources.</td>
</tr>
</tbody>
</table>

### 6 References


[34] Internet Engineering Task Force. An Architecture for Differentiated Services, S.


7 Exhibit X
Not Applicable.

8 Appendix
Not Applicable.
ACKNOWLEDGEMENTS

The National Emergency Number Association (NENA) 911 Core Services Committee, ESInet-PSBN Interconnection Working Group developed this document.

NENA Board of Directors Approval Date: **10/14/2021**

NENA recognizes the following industry experts and their employers for their contributions to the development of this document.

<table>
<thead>
<tr>
<th>Members</th>
<th>Employer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steve O’Conor, ENP, 911 Core Services Committee Co-Chair</td>
<td>Next Generation 9-1-1 Consulting Services, LLC</td>
</tr>
<tr>
<td>Terry Reese, 911 Core Services Committee Co-Chair</td>
<td>Ericsson</td>
</tr>
<tr>
<td>Michael Smith, WG Co-Chair</td>
<td>Equature/DSS Corp.</td>
</tr>
<tr>
<td>William Mertka, WG Co-Chair</td>
<td>Synergem Technologies Inc.</td>
</tr>
<tr>
<td>Aimee Chase ENP</td>
<td>Metro Communications Agency</td>
</tr>
<tr>
<td>Doug Cunningham</td>
<td>CenturyLink Inc.</td>
</tr>
<tr>
<td>Michael DeAngelo</td>
<td>Motorola Solutions, Inc.</td>
</tr>
<tr>
<td>Doug deGraaf</td>
<td>Benton County WA</td>
</tr>
<tr>
<td>Shelly Guenther, ENP</td>
<td>Guenther and Associates</td>
</tr>
<tr>
<td>Tim Hannah</td>
<td>South Sound 911 WA</td>
</tr>
<tr>
<td>Rob Howard</td>
<td>NYC3 Cyber Command</td>
</tr>
<tr>
<td>Tim Kenyon-ENP</td>
<td>AirOne Solutions Group LLC</td>
</tr>
<tr>
<td>James Kinney</td>
<td>INdigital</td>
</tr>
<tr>
<td>Steve Lagreid</td>
<td>King County WA</td>
</tr>
<tr>
<td>Jared Lamere</td>
<td>Vermont Enhanced 911 Board</td>
</tr>
<tr>
<td>Sean Lehman, GISP, ENP</td>
<td>GeoComm Inc.</td>
</tr>
<tr>
<td>Travis LePage, ENP</td>
<td>Federal Engineering, Inc.</td>
</tr>
<tr>
<td>Julie Lobb</td>
<td>Carbyne, Inc.</td>
</tr>
<tr>
<td>Roger Marshall</td>
<td>Comtech Telecommunications Corporation</td>
</tr>
<tr>
<td>Steve McMurrer, ENP</td>
<td>Fairfax County VA</td>
</tr>
<tr>
<td>Dave Pinsker</td>
<td>Northrop Grumman</td>
</tr>
<tr>
<td>Pierce Power, ENP</td>
<td>Teleira</td>
</tr>
<tr>
<td>Brian Rosen</td>
<td>Brian Rosen Technologies LLC</td>
</tr>
<tr>
<td>Ed Roth</td>
<td>Larimer Emergency Telephone Authority CO</td>
</tr>
<tr>
<td>Tina Thompson</td>
<td>Western Arkansas Planning &amp; Development District (WAPDD)</td>
</tr>
<tr>
<td>Jeffrey Wheeler</td>
<td>Data Technical Services</td>
</tr>
</tbody>
</table>
Special Acknowledgements:

Delaine Arnold, ENP, Committee Resource Manager, has facilitated the production of this document through the prescribed approval process.

The ESInet-PSBN Interconnection Working Group is part of the NENA Development Group that is led by:

- Jim Shepard, ENP, and Wendi Rooney, ENP, Development Steering Council Co-Chairs
- Roger Hixson, ENP, 9-1-1 Services Senior Consultant
- Brandon Abley, ENP, Technical Issues Director
- April Heinze, ENP, Operational Issues Director